REMARKS

In the office action dated 8/24/05, the Examiner rejected claims 1-7, 11, 12 and 14-19 as obvious over Jorgensen in view of Chiu et al.

Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention absent some teaching, suggestion or incentive to do so. In re Bond, 910 F.2d 831, 834, 15 USPQ2d 1566, 1568 (Fed. Cir. 1990). Suggestion arises from one of ordinary skill in the art perceiving a liklihood of success in solving the problem the inventors solved by making the combination. In other words, the consistent criterion for determination of obviousness is whether the prior art would have suggested to one of ordinary skill in the art that this process should be carried out *and would have a reasonable likelihood of success, viewed in the light of the prior art.* See Burlington Industries v. Quigg, 822 F.2d 1581, 1583, 3 USPQ2d 1436, 1438 (Fed.Cir.1987); In re Hedges, 783 F.2d 1038, 1041, 228 USPQ 685, 687 (Fed.Cir.1986).

It appears that the Examiner may be misinterpreting the claimed invention from the Examiner's statement at page 3 of the office action that "Jorgensen does not disclose **monitoring** of the links over which IPSEC transmission between a source and destination ...Chiu disclosed **congestion and flow control detection (monitoring)** of the communication links in a network...." (emphasis ours). This is a different problem than the problem solved by the invention.

Here, the problem the inventors solved was how to **measure the performance** of an IPSEC private tunnel communication link when neither the IPSEC protocol nor the TCP/IP protocol provides a way to monitor and measure the performance of an IPSEC tunnel. This is a useful feature because often multiple private tunnel data paths taking different routes through different gateways, different ISPs and different legs and routers on the internet are available to send data from a first node to a second node.

This problem is basically solved by sending special IPSEC acknowledgment packets back from the destination node to the source node in response to receipt of an IPSEC packet from the source node if either one of two conditions are satisfied. Each IPSEC acknowledgment packet contains the sequence number of the IPSEC packet just received and may contain a counter value indicative of the amount of data received in some embodiments. These ack packets are not the ack packets generated in the TCP/IP

protocol and they have a special data structure in that they contain at least the sequence number of the IPSEC packet received just before the IPSEC acknowledgment packet was sent. Specification, page 6, lines 9-17.

The two conditions under which an IPSEC acknowledgment packet will be sent are: 1) an IPSEC acknowledgment packet will be sent every Nth IPSEC packet received (Specification, page 6, lines 11-13); and 2) reception of an IPSEC packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet (Specification, page 6, lines 18-23).

Claim 1 Distinction Over The Prior Art

The transmission of these IPSEC acknowledgment packets is recited in claim 1 in the following language:

> - transmitting an acknowledgement packet by the destination network node ~~if~~ at least when a second condition ~~one~~ of a first condition and a second condition is fulfilled, said first condition being the reception of at least a predetermined number of IPSEC packets after transmission of the previous acknowledgement packet, and said second condition being the reception of an IPSEC packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet.

The claim limitation "transmitting an acknowledgment packet" should be interpreted as requiring generation of an IPSEC packet containing at least the sequence number of the IPSEC packet received to which the transmission of the acknowledgement packet is a response. A limitation in a claim should be interpreted in accordance with the specification and prosecution history, and to do so is not reading limitations into the claim. Under a recent *in banc* decision of the Federal Circuit, claim construction is a job for the judge as it is a question of law. Markman v. Westview Instruments, Inc., 52 F.2d 967 (Fed. Cir. 1995). Three intrinsic sources of data on this subject are the specification, the language of the claims themselves and the prosecution history. The judge is free to consider extrinsic sources also such as expert testimony, dictionaries, prior art references etc., but in the recent Vitronics decision, the Federal Circuit held that the meaning of the claims is almost always ascertainable from the intrinsic evidence and resort to extrinsic evidence is the exception rather than the rule. Vitronics Corp. v. Conceptronic Inc., 39 USPQ2d 1573 (Fed. Cir. 1996). Further, Vitronics holds that it is legal error to rely on extrinsic evidence where the meaning of the claims is clear from the intrinsic evidence.

It is always necessary to review the specification to determine whether the inventor has used any terms in a manner inconsistent with their ordinary meaning. The specification acts as a dictionary when it expressly defines terms used in the claims or when it defines terms by implication. The specification contains a written description of the invention which must be clear and complete enough to enable those of ordinary skill in the art to make and use the invention. Thus, the specification is always relevant to the claim construction analysis. Usually it is dispositive; it is the single best guide to the meaning of a disputed term. Vitronics Corp. v. Conceptronic Inc., 39 USPQ2d 1573, 1577 (Fed. Cir. 1996). If the specification does not give a term a unique or special meaning, the term will be given its ordinary meaning to one of skill in the art. Ekchian v. Home Depot Inc., 104 F.3d 1299, 41 USQP2d 1364 (Fed. Cir. 1997). The Federal Circuit has held that a patentee is bound by the specification in interpreting his claims even when the specification requires a narrower interpretation of the claims than the patentee desires. Fonar Corp. v. Johnson & Johnson, 821 F.2d 627, 3 USPQ2d 1109 (Fed. Cir. 1987). A narrower definition derived from the specification and prosecution history will prevail over a broader dictionary definition. Texas Instruments Corp. v. Cypress Semiconductor Corp, 90 F.3d 1558, 39 USPQ2d 1492 (Fed. Cir. 1996); Greiner v. Mari-Med, 962 F.2d 1031, 22 USPQ2d 1526 (Fed. Cir. 1992). Further, where a meaning for a claim term gleaned from the only embodiment taught in the specification is narrower and more specific than the general dictionary definitions of the words used in the claim, the meaning gleaned from the specification controls. Toro Co. v. White Consolidated Industries, Inc., 53 USPQ2d 1065, 1069 (Fed. Cir. 1999).

Here, the term acknowledgment packet in the claim is broad and reads on both IPSEC acknowledgment packets and TCP/IP acknowledgment packets. However, the specification defines the acknowledgement packet as having special content that a TCP/IP acknowledgment packet does not have in the following passage from page. 6, lines 10 et seq.

> In the method, the monitoring is effected by arranging the destination network node to send an acknowledgement packet for every N:th IPSEC packet received from the originating network node. The acknowledgement packet comprises at least a sequence number of the IPSEC packet, after which the acknowledgement packet is sent. The sequence number of an IPSEC packet is present in the ESP (enhanced security payload) or in the AH (authentication header) header, as described in the corresponding RFC documents and well known by a man skilled in the art. In a further advantageous embodiment of the invention, sending of an

> acknowledgement packet is caused also by reaching a certain time limit. In such an embodiment, if more time than a predefined limit T has elapsed after the previous acknowledgement packet has been sent, an acknowledgement packet is sent immediately when an IPSEC packet is received even if less than N packets have been received. That is, the fulfillment of either criterion - reception of more than N packets or elapsing of time T after sending of the previous acknowledgement packet - causes the sending of an acknowledgement packet

The Summary of the Invention at page 2, lines22-23 also teaches that it is preferable to include a counter value indicating the number of received IPSEC packets and/or the number of bytes received from that link so as to allow the determination of the packet success rate and/or throughput of the link. From these passages, it is clear that the acknowledgment packet called for by the claims must have at least the sequence number of the IPSEC packet received just before the acknowledgement packet is sent. TCP/IP packets do not have this content nor is there any need identified in the teachings of Chiu for them to have this content so there is no suggestion that they have this content.

Further, to interpret the term "acknowledgement packet" in the claims as reading on a TCP/IP acknowledgment packet makes no sense. This is because TCP/IP acknowledgment packets require as part of their content a TCP/IP protocol sequence number which is in the header of the TCP/IP packet, and this header is encrypted along with the rest of the TCP/IP packet in the payload section of the IPSEC private tunnel packet. To send a TCP/IP acknowledgement packet from the tunnel gateway upon receipt of an IPSEC packet would be impractical because the payload section of the IPSEC packet would have to be decrypted.

Therefore, the only interpretation that makes sense is the IPSEC acknowledgment packet interpretation from the specification, and the possible other interpretation lends enough indefiniteness to the claim to invite interpretation in light of the specification. Where the claim terms chosen are not defined in the claim and are of such a broad nature as to render the meaning of the claim indefinite, such claim terms invite resort to the specification to clarify their meaning. Johnson Worldwide Associates Inc. v. Zebco Corp., 50 USPQ2d 1607, 1610 (Fed. Cir. 1999). However, where the meaning of claim terminology is "sufficiently clear" in the patent specification, that meaning will prevail over a broader dictionary definition.

The Examiner states in his office action that it is the "concept" of an acknowledgement packet that he is taking from the Chiu reference in support of his

rejection. This argument is not legimate in U.S. patent law to support this obviousness rejection because it is based upon hindsight. The "concept" of claim 1 is to measure the performance of an IPSEC link using a special IPSEC acknowledgement packet sent under special conditions. This is an entirely different concept than is taught by Chiu which is concerned with how to make a TCP/IP multicast reliable **and not with how to measure the performance** of the TCP/IP multicast link. Reliability, as taught in Chiu, is just how to make sure all the packets got there. Performance as taught in the invention is about round trip times and throughput so that inbound and outbound ISP selections can be intelligently made (specification, page 5, lines 10-31). Thus, for the Examiner to select the acknowledgement packets out of the teaching of Chiu (especially where Chiu teaches its protocol is not compatible with IPSEC) **and for the Examiner to put these different ack packets which are used for different purposes into a facsimile of the invention is the exercise of hindsight.**

The prior art combination does not contain a teaching of generating special IPSEC acknowledgment packets which contain the sequence number of the IPSEC packet just received and sending it back from the destination node to the source node if either of the two conditions are satisfied. Specifically, Jorgensen teaches a virtual private network using a wireless PTMP transmission system which uses IPSEC as a method of security encryption. Jorgensen does teach using IPSEC protocol to tunnel IP packets on a communication link between a source network node and a destination network node. But the Examiner admits that Jorgensen does not teach monitoring the IPSEC protocol link in a manner as claimed in the present invention. The Examiner then asserts that it would have been obvious to modify the teachings of Jorgensen using the teachings of Chiu to achieve the claimed invention. Incorporating the teachings of Chiu into the system of Jorgensen would not solve the problem the inventors solved of how to measure the performance of an IPSEC link.

Jorgensen does not teach the generation and sending of IPSEC acknowledgment packets which contain the sequence number of the IPSEC packet just received.

Chiu does not teach generation of special IPSEC acknowledgment packets each of which contains the sequence number of the IPSEC packet just received and sending those IPSEC acknowledgment packets back from the destination node to the source node under one of the two conditions recited in claim 1.

Chiu is addressed to the problem of how to make a TCP/IP multicast reliable without

flooding the sending node with TCP/IP ACK and NACK packets from all the numerous destination nodes in the multicast. Chiu solves this problem by teaching a heirarchical structure comprised of a source node and a plurality of "repair heads" each of which talks to a plurality of destination nodes or member stations in the multicast. Chiu teaches use of the ACK windows and assignment of specific ACK windows to specific member stations (destinations) for timing of transmissions of the ACK messages to spread out the transmission of ACK and NACK messages and avoid flooding. Specifically, Chiu teaches at Col. 7, lines 11 - 37:

> The invention avoids an ACK implosion by spreading out the ACK (and NACK) messages so that a flood of them do not reach the repair head simultaneously. The use by members of the ACK window for timing of transmission of the ACK messages helps to prevent too many ACK messages from reaching the transmitting station at the same time. The ACK messages contain both acknowledgment information for packets received by the member station, and contain NACK information for packets not received by the member station, as based on the sequence numbers of the packets. The term "ACK message" will be used throughout this patent to indicate a message returned by a receiving station to a transmitting station, where the message carries both ACK and NACK information.
>
> The ACK window is defined for a multicast session by establishing the number packets which make a full sequence of ACK windows. Receipt of a full window of packets is an event which triggers transmission of an ACK message by a member station. In a preferred embodiment of the invention, the ACK window size is configurable, and the default number of packets which make a full sequence of ACK windows is thirty two (32) packets.
>
> To prevent many member stations from sending ACK messages at the same time, ACK messages are distributed over the next ACK window. Each member is assigned a window (for example between 1 and 32) for sending its ACK messages.

The ACK and NACK packets Chiu is talking about are TCP/IP ACK and NACK packets. Specifically, at Col. 4, lines 17-67 to Col. 5, line 25 Chiu teaches:

> The TCP portion of TCP/IP (The Connection Protocol) is a layer 4 protocol and establishes reliable communication between the end stations by causing retransmission of packets using the IP protocol.
>
> In a commonly used terminology, the words "datagram" and "message" are often used interchangeably. In an alternative usage, a "message" may be broken into one or more "datagrams". However, in this document the words "datagram" and "message" and "packet" are used interchangeably. A "frame" is used as the messaging unit transferred by the physical layer on a hop between two computers.
>
> Unreliable multicast communication is relatively simple to implement, as the source station simply transmits the datagrams with an address that the designated computers can recognize as a multicast address, and which routers forward. The

destination stations then receive any datagrams which they detect. No attempt is made to either identify or retransmit lost datagrams.

Reliable multicast is more difficult to implement. For example, in the case of a few destination computers, the source station must maintain a record of the ACK messages received from each intended destination station so that a datagram missing from any one of the destination stations can be retransmitted. However in the case where there are tens of thousands, even millions, of intended destination stations, the large number of ACK messages will flood the source station and will flood the network. The detrimental effect of too many ACK and too many NACK messages is referred to as ACK implosion or NACK implosion. Administration problems also arise, where for example, a source station has a particular destination station on its list of intended destination stations, and for some reason that destination station is no longer operational. The source station may then continue indefinetly retransmitting messages while waiting for an ACK from the missing station.

One solution to the reliable multicast problem, where the multicast message is to be received by a group of destination computers, has been to have an administrator (a person or a computer program operated by the person) set up a repair tree. In a repair tree, certain computers are designated as a "repair head". The rest of the computers of the group of destination computers are assigned to a designated repair head. Typically, a source station transmits a multicast datagram onto the network. The datagram should be received by all members of the destination group. Since the datagrams carry a sequence number, each destination station determine if it has missed a datagram. Each station sends an ACK to its repair head upon successful reception of a window of datagrams, and sends a NACK to its repair head upon determining that it has missed a datagram. Upon receipt of an ACK from every member of its repair group, the repair head flushes the datagram from its cache. The repair head retransmits any datagram for which it receives a NACK, until all members of its repair group respond with an ACK for each datagram.

In the event that a repair head is missing a datagram, it NACKs to the source station, and the source station retransmits the datagram. The source station maintains a cache of transmitted datagrams and flushes them after receipt of an ACK from each of the repair heads affiliated with the original source station.

Congestion on the network can result from large numbers of ACK and NACK messages. Particularly, a destination station which is slower than the transmitting source station will miss many multicast datagrams. The resulting NACK messages can cause a NACK implosion and contribute to network congestion. Upon receipt of a NACK message, a source station or repair head will begin retransmission of datagrams, thereby contributing to even more congestion. Congestion can particularly increase when a low bandwidth link is responsible for a number of destination stations being slower than the source station. Each destination station will miss numerous datagrams, and will flood the network with NACK messages, followed by more retransmissions in a feedback cycle which increases congestion.

The Examiner stated it would be obvious to modify the network teachings of

Jorgensen by using the method of monitoring a link through the transmission of ACK packets as disclosed in Chiu. In the Examiner's rejection, it is apparent he is relying upon the Chiu teaching of TCP/IP ACK and NACK packets as a teaching of the IPSEC acknowledgment packets of properly interpreted claim 1.

The prior art is missing a critical piece of knowledge needed to solve the problem the invention solved. Chiu is silent on the generation of special IPSEC acknowledgement packets which contain the sequence number of the IPSEC packet just received. This is a key claim feature required to solve the problem the inventors solved, and it is completely missing from the prior art combination.

Where the prior art of a combination of references cited in support of an obviousness rejection does not teach an element needed to solve the problem the claimed invention solved, the obviousness argument must fail. In re Hayes Microcomputer Products, Inc., 982 F.2d 1527, 1541, 25 USPQ2d 1241 (Fed. Cir. 1992) [failure of prior art to teach a claimed method of detecting escape sequences in modems doomed obviousness invalidity argument of infringer even though escape sequences themselves were admittedly in the prior art]. There is no suggestion to support an obviousness rejection based upon a combination of references where the combination of references does not contain all the knowledge needed to make the claimed invention.

Further, there are practical difficulties in modifying Jorgensen with the teachings of Chiu which negate suggestion to make the modification and undercut the viability of the obviousness rejection. As mentioned above in the section on the proper interpretation of "acknowledgment packet", TCP/IP acknowledgment packets require as part of their content a sequence number which is in the header of the TCP/IP packet, and this header is encrypted along with the rest of the TCP/IP packet in the payload section of the IPSEC private tunnel packet. To send a TCP/IP acknowledgement packet from the tunnel gateway upon receipt of an IPSEC packet would be impractical because the payload section of the IPSEC packet would have to first be decrypted and the sequence number in the TCP/IP packet obtained and put in a TCP/IP ACK packet. The TCP/IP packet which would then have to re-encrypted and encapsulated in an IPSEC packet and sent back to the source. There the encapsulated TCP/IP packet would have to be decrypted and the sequence number recovered. Chiu does not teach storing transmission times of the TCP/IP packets to which the TCP/IP ACK and NACK packets are a response. Therefore, calculation of round trip time would not be possible as a form of monitoring. One skilled in

the art would reject this approach as too awkward, too slow and lacking in the ability to calculate round trip time which is an important thing to know in monitoring an IPSEC tunnel, especially where several different possible IPSEC tunnels exist and the fastest one is a fact of interest. The Federal Circuit in In Re Newell, 891 F.2d 899, 13 UAPQ2d 1248 (Fed. Cir. 1989) reversed an obviousness rejection upheld by the Board stating:

> "The motivation to make a specific structure is not abstract, but practical, and is always related to the properties or uses one skilled in the art wold expect the structure to have if made."

891 F.2d at 901, 13 USPQ2d at 1250

Here, the practical difficulties of trying to use TCP/IP ACK and NACK packets between endpoints of a secure IPSEC tunnel which is sending IPSEC packets encapsulating packets of another protocol such as TCP/IP would discourage one of skill in the art from attempting to make the combination proposed by the Examiner. If the combination or modification suggested by the Examiner were to be made, it either would not work at all or would not work well. This is the antithesis of suggestion. It is teaching away from the combination.

A reference may be said to teach away from a proposed combination in support of an obviousness rejection when a person of ordinary skill in the art, upon reading the reference, would be led in a direction divergent from the path that was taken by the applicant to solve the problem the claimed invention solved or would be discouraged from using the teachings of the reference in attempting to solve the problem the claimed invention solved. In re Gurley, 27 F.3d 551, 553, 31 USPQ2d 1130, 1131 (Fed. Cir. 1994). In general, a reference will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the applicant. 27 F.3d at 533, 31 USPQ2d at 1131. References taken in combination teach away when they would produce a "seemingly inoperative device". 27 F.3d at 553, 31 USPQ2d at 1131-1132. In re Caldwell, 319 F.2d 254, 256, 138 USPQ 243, 245 (CCPA1963) (reference teaches away if it leaves the impression that the product would not have the property sought by the applicant).

Here, an attempt to use the teachings of Chiu in using TCP/IP ACK and NACK packets to modify Jorgensen to monitor the performance of the IPSEC tunnel of Jorgensen would seem to yield an inoperative device and method or at least a device and method which would not have the properties sought by the applicant. Support for this

argument can be found in the Chiu reference itself at Col. 35, lines 11-52. There, addressing the issue of security, Chiu mentions that sender authentication in a TCP/IP mutlicast can possibly be solved using IPSEC protocol or digital signatures in the data messages generated by the sender. However, Chiu teaches that his TRAM protocol is not compatible with any of the security possibilities he mentions and that a security layer must be implemented above the TRAM protocol layer. This means that the TRAM protocol cannot be used with IPSEC tunnels, and this teaches away from combining the TRAM protocol teachings with the Jorgensen IPSEC tunnels.

In other words, the combination of Chiu and Jorgensen would be inoperative. This is because the key to solving the problem is in sending IPSEC ack packets which contain the sequence number of the IPSEC packet just received at the destination node. Chiu teaches using TCP/IP ACK and NACK packets to make TCP/IP multicast reliable. Even if IP packets are tunnelled in the IPSEC tunnel, the TCP/IP packets are encrypted so the sequence numbers of the received TCP/IP packets are not available to the endpoint nodes of the IPSEC tunnel. The only way the Chiu protocol would work would be behind the IPSEC tunnel endpoints where the IP packets have been recovered and their sequence numbers are available for retrieval and putting in TCP/IP ack packets. But these are not the sequence number of IPSEC packets so the throughput and round trip times of the IPSEC tunnel itself could not be determined using the Chiu ACK and NACK packets. The throughput of the IPSEC tunnel is the number of IPSEC packets received per unit of time. The round trip time is the time from transmission of an IPSEC packet from a source and the time of reception by said source of the IPSEC ack packet sent in response to receipt of the IPSEC packet transmitted by the source. The Chiu TRAM protocol, even if combined with the Jorgensen IPSEC tunnel, would not provide enough information to determine either the round trip time or the throughput of the IPSEC tunnel itself.

The Jorgensen-Chiu combination would also not have the properties sought by the applicant because Chiu does not teach sending an acknowledgement packet if either of the two conditions recited in claim 1 are true. Therefore, even if the combination of Chiu and Jorgensen could be made and there is no technological incompatibility, the claimed combination still would not perform the same functions as recited in claim 1, *i.e., sending an acknowledgement packet if either a predetermined number of IPSEC packets have*

been received or if an IPSEC packet has been received after a predetermined time has elapsed from transmission of the last acknowledgement packet.

Chiu is also directed to a different problem than the claimed invention and does not recognize the problem sought to be solved by the applicants. Specifically, Chiu teaches that the TCP flow control mechanism of ACK and NACK packets should be used to make TCP/IP multicasts reliable. He does not recognize that there is no flow control in IPSEC tunnels, and one skilled in the art reading Chiu would perceive no need for additional flow control since the Chiu TRAM protocol already teaches flow control so one skilled in the art would ask himself or herself why would any additional flow control be necessary. Even if the need for flow control in an IPSEC tunnel were perceived, one skilled in the art would reject the TRAM protocol as a way of doing it because Chiu teaches in Col. 35 that his protocol is not compatible with IPSEC. One skilled in the art would believe this since Chiu depends upon TCP ACK and NACK packets which include sequence number of the TCP/IP packets. These sequence numbers are not available at the IPSEC tunnel protocol level because the encapsulated TCP/IP packet is encrypted.

This raises a further reason why one skilled in the art would reject the notion of combining Chiu with Jorgensen. Chiu teaches the need for and a mechanism to reduce overhead signalling on the network while still making multicast reliable by using repair heads. To use Chiu's TCP ACK and NACK packets inside an IPSEC tunnel would require either additional signalling to send the TCP/IP packet sequence numbers in the clear so that could be incorporated into the TCP ACK and NACK packets, or additional processing to decrypt the encapsulated TCP/IP packets in the received IPSEC packets would be required. Chiu teaches simplifying and reducing overhead signalling, not increasing complexity or increasing overhead signalling.

So Chiu provides a different solution (use of repair heads in a tree structure and scheduling of TCP/IP ACK and NACK packets to avoid flooding) than is required to solve the problem of the invention. The environment in which the invention operates is an IPSEC tunnel which has two endpoints. This is not the multicast environment of Chiu and there are no hierarchically structured repair heads which receive scheduled TCP/IP ACK and NACK packets so as to retransmit missing packets so as to make the multicast reliable without flooding the sender with TCP/IP ACK and NACK packets.

If the applied prior art does not indicate any awareness of the problem solved by

the applicants, it is hardly fair to take the position the Examiner has taken that one skilled in the art would perceive suggestion to use the teachings of the reference to solve the problem solved by the claimed invention. In re Nomiya, 509 F.2d 567, 184 USPQ 607 (CCPA 1975). There must, however, be a reason apparent at the time the invention was made to the person of ordinary skill in the art for applying the teaching at hand [to solve the problem the applicants have solved], *or the use of the teaching as evidence of obviousness will entail prohibited hindsight.* Graham v. John Deere Co., 383 U.S. 1, 36, 86 S.Ct. 684, 15 L.Ed.2d 545 (1966).

Invention can lie in the discovery of the source of the problem even with the solution is simple once the source of the problem is discovered. In re Nomiya, 509 F.2d at 571. In Nomiya, the problem solved by the invention was discharge of data of memory cells of a memory circuit with very low capacitance when an IGFET switching transistor with a protective diode is used to store the data or to input signals. The protective diode formed in the same substrate as the IGFET prevent breakdown of the thin oxide gate insulation layer when charge buildup on the gate occurs. The protective diode of the prior art prevented a sufficiently high voltage buildup on the gate to cause punch through of the gate oxide. Unfortunately, it also created a small parasistic bipolar transistor formed between the protective diode and the drain of the IGFET when the protective diode was forward biased by a noise signal. This caused a spontaneous drainage of the stored charge out through the drain region and destroyed the operation of the memory cell. The solution to this problem was formation of a second protective diode outside the substrate.

The cited prior art in support of the obviousness rejection taught a protective diode in an improved IGFET **but did not recognize that the protective diode could lead to parasitic transistor action that could destroy proper operation of the cell.**

The CCPA held that the failure of the prior art to recognize the problem realized by the inventors was fatal to the obviousness rejection because the obviousness rejection was based upon hindsight reconstruction using the teachings of the applicant to view the prior art. The CCPA noted that there would have been no suggestion in the prior art teaching of a protective diode to add a second protective diode which is outside the substrate. This is because the second diode would be deemed to be superfluous since a first protective diode already existed and the prior art, not recognizing the source of the problem, would not recognize the need for a second protective diode formed outside the

substrate in which the IGFET was formed. In Judge Rich's inimitable and clear fashion, the CCPA held:

> "If, as appellants claim, there is no evidence of record that a person of ordinary skill in the art at the time of appellants' invention would have expected the problem in the IGFET to exist at all, it is not proper to conclude that the invention which solves this problem, which is claimed as an improvement of the prior art device... would have been obvious to that hypothetical person of ordinary skill in the art."

509 F.2d at 572, 184 USPQ2d at 613.

Here, neither Jorgensen nor Chiu recognize the need for monitoring the performance of an IPSEC tunnel. Chiu is concerned with making an IP Multicast transport mechanism reliable without flooding the sender with TCP/IP ACK and NACK packets. The TCP/IP ACK and NACK packets are used only by the repair heads to figure out which packets need to be resent to various destinations. This is taught in Chiu at Col 17, lines 21-42 where Chiu teaches the TCP ACK and NACK packets contain the TCP/IP packet sequence number of the first missing TCP packet so that this packet can be resent. That is not the same as sending in an IPSEC ack packet the sequence number of the last IPSEC packet received so that the sender can use the sending time of that IPSEC packet (as identified by the sequence number in the IPSEC ack packet) and the reception time of the IPSEC ack packet sent in response to reception thereof to calculate round trip time through the IPSEC tunnel.

IPSEC packet sending times are not stored in Chiu (nor are TCP/IP packet sending times) so round trip time cannot be calculated in Chiu and there is no mention of the two conditions for sending an IPSEC ack packet recited in claim 1. That is why the teachings of Chiu regarding sequence number and the lack of teaching of storing sending times would suggest to one skilled in the art that Chiu's TRAM protocol cannot be used to calculate round trip times in an IPSEC tunnel to monitor its performance. Since neither Jorgensen nor Chiu recognize a need to monitor IPSEC tunnel performance, neither suggest combination with the other to solve this problem.

Finally, even if the combination could be accomplished technically, which appears to not be the case, the combination would still fall short of the solution the applicants have provided since there is no teaching of IPSEC ack packets with the sequence numbers of the IPSEC received packets in them or the two conditions under which the IPSEC ack packets are sent. The Examiner cited Chiu Col. 16, lines 63-67 as teaching transmitting the ACK packet if at least one of two conditions are satisfied. This is a

misreading of Chiu since that section teaches a TCP ack window and sending a TCP ACK packet after one TCP window of packets has been received. This is not the same as counting the number of IPSEC packets received since transmission of the last IPSEC ack packet and the jump from TCP ACK windows to counting IPSEC packets results from the use of hindsight reconstruction since Chiu teaches his protocol is not compatible with IPSEC.

The Examiner refers to Chiu Col. 17, lines 21-42 as teaching an ack packet comprises at least the sequence number of the last received IPSEC packet and at least one value corresponding to the amount of data received via the link. This is a misreading of that passage. **At Col. 17, lines 21-42 Chiu teaches the TCP ACK and NACK packets contain the TCP/IP packet start sequence number and a bit map length. Chiu teaches that if no packets were missing, the bit map length is zero, and the sequence number included in the ack packet indicates that all packets prior to and including this packet were successfully received. If one or more packets were not received, the sequence number indicates the first missing packet that must be resent and a bit map will follow that indicates which packets must be resent. The data in the ack packet and the bit map are for determining which packets are to be resent, not a measure of the throughput in terms of packets successfully sent per unit of time.**

These teachings are not the same as sending in an IPSEC ack packet the sequence number of the last IPSEC packet received so that the sender can use the sending time of that IPSEC packet (as identified by the sequence number in the IPSEC ack packet) and the reception time of the IPSEC ack packet sent in response to reception thereof to calculate round trip time through the IPSEC tunnel.

Independent claim 2

Independent claim 2 contains the following limitations that distinguishes it over the combination of Jorgensen and Chiu:

> - transmitting *an acknowledgement packet by the destination network node ~~if~~ at least when a second condition ~~one~~ of a first condition and a second condition is fulfilled, wherein said acknowledgement packet comprises at least the sequence number of the last received IPSEC packet* **and at least one value corresponding to the amount of data received via the IPSEC communication link**, said first condition being the reception of at least a predetermined number of IPSEC packets after transmission of the previous

acknowledgement packet, and said second condition being the reception of a packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet.

The italicized limitations should be interpreted the same way as the corresponding limitation in claim 1. The argument for non obviousness given above for claim 1 is hereby incorporated by reference.

The limitation set off in bold is another element of knowledge that is not present in the combination of Chiu and Jorgensen. Chiu teaches the content of the TC/IP ACK messages he uses at Col. 7, lines 16-20 as containing both acknowledgment information for packets received by member stations and NACK information for packets not received by the member stations, as based upon the seqence numbers of the packets. Chiu also teaches inclusion of a bit map in the TCP acknowledgement packet, but this bit map is not for purposes of calculating how much data was received. Instead, it is included to calculate exactly which packets need to be resent starting from the sequence number of the first missing TCP packet.

Therefore, there is no teaching of an ACK packet in Chiu which contains a "value corresponding to the amount of data received via the IPSEC communication link". Since Chiu is not concerned with measuring the throughput of the channel, there is no need in the ACK packets of Chiu to contain a number indicative of the amount of data received via the channel. Chiu is only concerned about which packets were not received. Since Chiu does not recognize the problem of measuring the throughput of an IPSEC tunnel, his ACK packets do not suggest a solution since they do not contain the information needed to solve this problem.

Claims 3-7 all depend from claim 2 so they are not obvious for the same reason their parent claim is not obvious.

Independent Claim 11 Argument

Claim 11 contains the following limitations which distinguish it over the prior art combination of Jorgensen and Chiu:

- means for sending acknowledgment packets for said IPSEC packets containing IP packets,
- means for receiving said acknowledgement packets for said IPSEC packets,
- means for obtaining a sequence number of an IPSEC packet from said a received acknowledgement packet,
- means for obtaining a value from said the acknowledgement packet, said value corresponding to the amount of data received via the communication link by

said second network node, and

- means for determining the packet success rate of the communication link at least partly on the basis of said value.

The limitation:

- means for sending acknowledgment packets for said IPSEC packets containing IP packets,

is a means plus function limitation, and should be interpreted in accordance with 35 USC 112, Para. 6 to read on the apparatus recited in the specification to carry out the recited function of sending an ack packet for IPSEC packets containing an IP packet. Interpretation of means-plus-function claims is controlled by statute 35 U.S.C. 112, Para. 6. That statute states:

> "An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof."

Therefore, this limitation should be interpreted as requiring a computer programmed to carry out the function of sending an IPSEC acknowledgement packet under either one of the two conditions recited in the specification at page 20, lines 20-25 in response to receipt of an IPSEC packet containing a sequence number, said IPSEC acknowledgement packet containing the sequence number of the IPSEC packet just received and a value corresponding to the amount of data received. (specification page 20, lines 20-25 and lines 30-34, Figure 8, items 821, 822, 862, 874, 860, 870, page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, line 9 to page 10, line 7, Figure 6, step 620, page 15, lines 15-16, Figure 6, 620).

Since this limitation is the hardware superset equivalent of the method step of claim 1 of sending an IPSEC ack packet under the second of two conditions, all the same arguments recited above for non obviousness of claim 1 based upon this limitation are applicable here and are hereby incorporated by reference.

Claim 11 also contains the following additional limitations that are not found in the prior art combination:

- means for receiving said acknowledgement packets for said IPSEC packets,
- means for obtaining a sequence number of an IPSEC packet from said a received acknowledgement packet,
- means for obtaining a value from said the acknowledgement packet, said value corresponding to the amount of data received via the communication link by

said second network node, and

- means for determining the packet success rate of the communication link at least partly on the basis of said value.

Chiu does not teach receiving IPSEC acknowledgement packets sent in response to reception of IPSEC packets and extracting both a sequence number of the IPSEC packet to which the ACK packet is a response as well as a value indicative of the amount of data received at the destination node. Chiu's TCP/IP ACK and NACK packets do contain sequence numbers of TCP/IP packets received so that the repair heads can figure out which packets were not received and re-send them to make the multicast reliable. However, there is no value in the TCP/IP ACK and NACK packets which is indicative of the amount of data received by the destination node since that is not part of the Chiu solution. **The bit map of Chiu only tells which packets were not received, and the undersigned believes that packets can vary in size in TCP/IP so the bit map is not data which indicates how much data was received**. Chiu does not recognize the need for determining the amount of data received, only the need for determining which exact data packets were received. In short, Chiu is not concerned with measuring packet success rate so his ACK packets and bit map do not contain the data needed to calculate packet success rate and he does not calculate packet success rate. As such, Chiu does not suggest modification of Jorgensen to generate IPSEC ack packets containing both sequence numbers and a value indicative of the amount of data received and to receive those IPSEC ack packets and use the aforementioned data to calculate packet success rate.

Dependent claim 12 depends from claim 13, so it is not obvious for the same reaons claim 12 is not obvious.

Independent Claim 14 and 15 Argument

Independent claims 14 and 15 are the means plus function hardware analog of claim 1 that covers apparatus in the specification that carries out the recited functions to implement a process like the process of claim 1. Both claims contain limitations in the form of means for transmitting acknowledgement packets at least when a second of first and second conditions occurs. The acknowledgement packets and the first and second conditions are the same as in claim 1. As such, claims 14 and 15 are not obvious over the combination of references applied to claim 1 for the same reasons recited above in the argument regarding claim 1.

Dependent claims 16 and 17 both depend from claim 15 and are not obvious for the same reasons claim 15 is not obvious.

Independent Claim 18 Argument

Independent claim 18 contains the following means plus function limitation which distinguishes it from the combination of Jorgensen and Chiu:

> - means for transmitting an acknowledgement packet ~~if~~ at least when a second condition ~~one~~ of a first condition and a second condition is fulfilled,
> said first condition being the reception of at least a predetermined number of IPSEC packets after transmission of the previous acknowledgement packet, and
> said second condition being the reception of a packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet,

This limitation is the hardware analog of the step of transmitting ack packets under at least a second of two conditions recited in claim 1 and is not obvious for the same reasons discussed at length above in the argument regarding claim 1.

In addition, claim 18 contains limitations regarding calculating the packet success rate from data included in the ack packet regarding the amount of data successfully received. As pointed out above, Chiu does not teach an ack packet or a bit map that includes data regarding how much data was received since the bit map only includes bits which correspond to packets that must be resent. These set bits in the bit map do not indicate the size of the packets that need to be resent.

Claims 14, 15 and 18 all contain limitations stated in means plus function form which require means for using an IPSEC protocol communication link to tunnel IP packets between a first and second node. In addition, each of these claims contains limitations stated in means plus function format which require a means for transmitting an acknowledgment packet if at least one of a first and second conditions is fulfilled. Per the specificaton sections cited above for other claims containing similar limitations about using IPSEC tunnels and sending acknowledgment packets when either of a first or second condition is present, these limitations should be interpreted under 35 USC 112, Para. 6 to require transmission of an IPSEC acknowledgment packet to the source node in response to receipt of an IPSEC packet, said ack packet being sent when either: 1) a predetermined number of IPSEC packets has been received by the destination node; or 2) receipt of an IPSEC packet after a predetermined timeout from transmission of the last IPSEC ack packet. The ack packet is an IPSEC packet which contains at least the

sequence number of the last IPSEC packet received.

Because these limitations are similar to the process limitations of claim 1 but are apparatus which perform these process steps, the argument given above for the nonobviousness of claim 1 based upon the similar process limitations is repeated here by incorporation by reference. If the prior art combination does not teach method steps to send these IPSEC ack packet or suggest sending such packets, it also does not teach a computer programmed to carry out this method.

In addition, claim 15 contains an additional limitation regarding inserting in the IPSEC ack packet a byte counter value which is indicative of the amount of data received. As noted above for other claims containing a similar process limitation, both Chiu and Jorgensen are silent on the need to include such a byte counter value in the ack packet since that value is used to calculate throughput or packet success rate, and neither end result is required in these references to solve the problems addressed by these references. The Examiner cites Col. 31, lines 50-61 of Jorgensen as teaching that the TCP protocol layer of the sender provides the TCP header for an IP packet with a byte number. This byte number is provided for purposes of reliable data flow so that the recipient can tell if all bytes have been received and send back ACK and NACK packets indicating which bytes need to be resent. In other words, the byte count of Chiu is conventional TCP technology that can be used to control retransmssion of missing bytes in a packet flow. It is not intended to provide any information about the amount of data received as called for by the claims being argued here.

Accordingly, neither of these references provides a suggestion to add such a value to an IPSEC ack packet. Therefore, suggestion to combine Chiu and Jorgensen to reach the invention claimed in claim 15 is lacking, and even if the references were to be combined, the result would still fall short of claim 15 and not have the same properties or achieve the same end result.

Claim 18, properly interpreted, calls for the sending an IPSEC ack packet with the sequence number of the last received IPSEC packet in it and a value indicative of the amount of data received. In addition, it contains means plus function limitations which, properly interpreted in accordance with the specification passages recited above for similar limitations in other claims, call for apparatus to receive the IPSEC ack packets, obtain the IPSEC packet sequence numbers and values indicative of the amount of data received from the ack packet and use that extracted data to calculate the packet

success rate.

Such an apparatus and method is not taught in either Chiu or Jorgensen because neither reference is addressed to the problem of measuring the performance of an IPSEC tunnel by calculating the packet success rate of transmission of transmitted IPSEC packets. Accordingly, there is no suggestion to one of skill in the art to apply the teachings of Chiu to modify the teachings of Jorgensen to extract the sequence numbers and volume of data number from the received IPSEC ack packets and calculate the packet success rate.

Independent Claim 19 Argument

Independent claim 19 is a computer-readable medium claim where the medium contains code with controls a network node to carry out a process which is the analog of claim 18. Claim 19 recites program code which sends an ack packet when at least a second of first and second conditions occurs and includes limitations about calculating the packet success rate from data about the volume of data received which is extracted from the ack packet. As such claim 19 is not obvious for the same reasons argued above for the non obviousness of claims 19 and 1.

Independent claim 19 is a software product claims that call for media having programmed thereon instructions that control a network node to implement an IPSEC tunnel to tunnel IP packets from a source node to a destination node, and send ack packets back to the source node if at least a second of a first or second condition is fulfilled. Properly interpreted, these claims define software code containing media which controls a computer to send IPSEC ack packets under either of the two conditions recited above. These limitations are similar to the limitations discussed above for process claim 1 in the non obviousness argument, but are stated in terms of program code which controls a computer to carry out the recited process steps which are similar to the process steps recited in claim 1. As such, the nonobviousness argument given above for claim 1 is repeated here by reference.

In addition, claim 19 further defines program code means which, properly interpreted in accordance with the specification passages recited above in the section entitled SUMMARY OF CLAIMED SUBJECT MATTER, controls a computer to receive IPSEC ack packets, extract IPSEC packet sequence numbers from them, and extract a value indicative of the amount of data received by the destination node, and calculate the packet success rate on the basis of the data extracted from the IPSEC ack packet.

Chiu is concerned with making a TCP/IP multicast reliable and teaches receiving TCP/IP ACK and NACK packets by the repair heads and then using the data in the TCP/IP ACK and NACK to resend packets in the multicast to destinations that indicated they did not receive them. No calculation of packet success rate is required for this process, and neither Chiu nor Jorgensen performs such a calculation. Accordingly, there is no suggestion to combine Chiu with Jorgensen to obtain code which controls computers to implement an IPSEC tunnel, send IPSEC ack packets which contain sequence number and volume data, receive the IPSEC ack packets and extract the sequence and volume data therefrom and calculate a packet success rate therefrom.

Independent Claims 8, 13 and 20 Argument

The Examiner has rejected claims 8, 13 and 20 as unpatentable over Jorgensen in view of Chiu as applied to claims 1-7, 11, 12, and 14-19 , and further in view of Alvisi et al. (US 20050027859).

The Examiner admits that neither Jorgensen or Chiu discloses dietermining the round trip time of the communication link on the basis of the reception time of an acknowledgement packet and the stored transmission time of the corresponding transmitted packet.

The Examiner points to paragraphs 68 and 69 of Alvisi as teaching calculation of a round trip time for a TCP protocol. What paragraphs 68 and 69 teach is that a round trip time is calculated in most connection oriented protocols such as TCP so as to calculate the retransmission timeout.

Claim 20 has all the limitations from claim 19 above except for extracting the volume information from the IPSEC ack packets and calculating the packet success rate. Claim 20 substitutes limitations defining computer code which controls the source node to store the sequence number and transmission time of each IPSEC packet sent in the IPSEC tunnel and receive IPSEC packets and calculate the round trip time of the IPSEC tunnel based upon reception time of the IPSEC ack packet and the stored transmission time of the IPSEC packet to which the IPSEC ack packet is a response. Since Chiu is not concerned with the round trip time of a single link in his reliable multicast protocol and he does not calculate round trip times in the multicast links, there is no suggestion to one of skill in the art to apply the teachings of Chiu to Jorgensen to arrive at code which controls a computer to use IPSEC ack packets and stored transmission times of IPSEC packets to which the IPSEC ack packets are a response to calculate round trip time of the link.

As noted before, Chu teaches to provide a reliable multicast transmission by means of the TCP protocol. Chiu explicitly states that a TCP portion of TCP/IP establishes reliable communication between the source and destination stations by causing retransmission of packets using the IP protocol. The same reliable TCP protocol is utilized in the multicast with the exception that the acknowledgements are transmitted to and the retransmissions are carried out by multiple repair heads in the network.

Thus, if a person skilled in the art had applied teachings of Alvisi in the system of Chiu, it would have resulted in calculation of round trip time for multicast TCP transmission in order to define retransmission timeouts. In other words, Alvisi would guide the skilled person to improve the TCP multicast protocol reliability and not to calculate round trip time in an IPSEC link so as to measure the performance thereof. Calculating retransmission times is not calculating the performance of a link , and Alvisi is devoid of any suggestion of a way to calculate round trip time on an IPSEC link.

Alvisi would not have motivated the person skilled in the art to make any arrangement in any hypothetical combination of Jorgensen and Chiu systems to measure the performance or throughput, or to calculate round trip time of the IPSEC link on the IPSEC level, in addition to the TCP flow control and error recovery.

Therefore, there is no suggestion in Alvisi to modify the combination of Jorgensen and Chiu to achieve the invention claimed in claims 8, 13 and 20 of measuring performance of an IPSEC communication link by calculating round trip time from the sequence numbers in IPSEC packets.

Claims 8 and 13 and 20 both contain limitations specifying that an IPSEC protocol is used to transmit IPSEC packets, IPSEC ack packets are sent (which contain sequence numbers of IPSEC packets), sequence numbers and transmission times of IPSEC packets are stored and that data plus the sequence numbers in the ack packets are used to calculate the round trip time. This combination of elements of knowledge is not present in the combination of Jorgensen, Chiu and Alvisi.

Claim 9 and 10 Argument

The Examiner has rejected claims 9 and 10 as unpatentable over Jorgensen in view of Chiuand Alvisi as applied to claim 8 and further in view of Tam and Garcia-Luna-Aceves. This rejection is a repeat of the rejection previously appealed except for the addition of Alvisi. The Examiner admits that neither Jorgensen, Chiu or Alvisi disclose monitoring of an inactive link between a source and destination as recited in claim 9.

Claim 9 contains the following limitation which distinguishes it over this prior art combination:

> said method comprising at least the following steps for monitoring an active communication link between the source network site and the destination network site, the active communication link employing the IPSec protocol:
>
> the step of transmission of an acknowledgement packet by the destination network node ~~if~~ at least when a second condition ~~one~~ of a first condition and a second condition is fulfilled,
>
> said first condition being the reception of at least a predetermined number of IPSec packets after transmission of the previous acknowledgement packet, and
>
> said second condition being the reception of a packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet,

This process step of transmitting a acknowledgement packet when at least a second condition of two conditions should be interpreted in the same way as the similar process step in claim 1 based upon the same intrinsic evidence recited above from the specification. The argument for nonobviousness of claim 1 is hereby incorporated by reference. The TAM teachings of sending probe packets over an inactive TCP/IP link do not alter the argument given above regarding the nonobviousness of claim 1 and other claims which contain a limitation like that cited above. The basic combination of Jorgensen and Chiu and Alvisi do not contain all the knowledge embodied in the quoted limitations and does not suggest the claimed invention. The teachings of Garcia of measuring link delays and replacing active links with inactive links based upon the result of monitoring, do not alter the argument given above regarding the nonobvious of claim 1 and other claims which contain a limitation like that cited above.

In addition to the above quoted limitation, claim 9 includes limitations regarding sending probe packets over inactive links and storing the transmission time of the probe packet and transmitting a response packet back to the source upon receipt of the probe packet and using the response packet reception time and the stored probe packet transmission time to calculate the round trip time of the inactive communication link and replacing the active link with the inactive link selectively based upon the round trip time calculation.

Notwithstanding the fact that the prior art combination does not teach probing the inactive links, calculating round trip times and selectively replacing the active link, the prior art combination also teaches away from sending IPSEC ack packets which contain IPSEC

packet sequence numbers under at least the second of two conditions. Further, the prior art combination of Jorgensen and Chiu would be inoperative and not have the desired properties needed to make the invention.

The prior art combination is still lacking the knowledge needed to make the invention including the limitations identified above. Tam teaches probing a TCP protocol communication link but does not teach monitoring an inactive IPSEC link between a source node and a destination node which has an active IPSEC link which is monitored at the same time. Further, neither Chiu nor Tam teach maintaining the present status of the active and inactive IPSEC links or replacing the active link with an inactive link based upon the results of the monitoring. Finally, neither Chiu nor Tam teach calculating the roundtrip time of the inactive link. All this is what claim 9 calls for.

Therefore, there is no suggestion to combine cited references to achieve the inactive link monitoring and substitution invention of claim 9. The addition of Tam and Garcia to this prior art combination does not change this conclusion. This is because neither of these prior art references teaches generation of IPSEC ack packets with sequence number of the IPSEC packet just received in an IPSEC tunnel, said ack packet being sent if at least a second of two conditions are met. Accordingly claim 9 is not obvious for lack of suggestion to make the proposed combination. Since claim 9 is not obvious, its more narrow dependent claim 10 is also not obvious.

Arguments In Response To Examiner's Response To Arguments In Appeal Brief

The Examiner admitted that the acknowledgement process of Chiu is applied specifically to TCP/IP, and he stated he was using the concept of the ack packet from Chiu in his rejection and not the specific TCP/IP version thereof. Thus, the Examiner had admitted there are no specific facts in Chiu that suggest that the TCP/IP ack packets there could be used in an IPSEC tunnel. In fact, Chiu teaches just the opposite, i.e., that his protocol is not compatible with IPSEC. **Therefore, for the Examiner to pluck the TCP/IP ack packet taught in the Chiu protocol out of Chiu and put it into an IPSEC environment is pure hindsight and does not legally support an obviousness rejection as there not only is no suggestion that this can or should be done but there is a specific teaching against it.**

The Examiner continues by saying:

"However, such an acknowledgement scheme would be beneficial to any

> other communication protocol. It is the opinion of the Examiner that it would have been obvious to one of ordinary skill in the art at the time of the invention to apply such an acknowledgement packet method, in which the ACK packet contains a sequence number, to other protocols including IPSec, to provide verifiable transmission as well as other information about communication link made available through the use of the acknowledgement packet scheme shown by Chiu."

The Examiner cannot support an obviousness rejection simply by his opinion in the fact of conflicting evidence from the prior art references applied. The prior art does not contain all the knowledge needed to make the invention. The prior art suggests that the Chiu protocol will not work in IPSec environments. The prior art suggests that even if Chiu were combined with Jorgensen, and the other references, the combinaton still would not work to measure the performance of an IPSEC link.

The Examiner goes on to interpret a disclosure of Chiu that an acknowledgemetn packet is sent to acknowledge a predetermined window of packets at a time, as sending an ack pcaket after a predetermined number of packets have been received, thus allegedly meeting the first condition recited in claim 1. It seems that the Examiner is concentrating only on the first condition and ignoring the second condition. The either-or structure of claim 1 prior to this amendment may be the reason for the Examiner ignoring the second condition because the either-or structure suggests alternative embodiments. This is the reason the claims have been amended to specify that the ack packet is transmitted by the destination network node at least when the second condition is fulfilled. The applicant urges the Examiner to adequately consider the second condition and allow the claims.

Finally, the Examiner again states that although Chiu and Jorgensen focus on apsects of communication different from those focused on by the Applicant, and at the time of the invention, no apparent reason exists to apply the teaching at hand, for monitoring the performance of an IPSEC tunnel, the scheme proposed by Chiu nonetheless demonstrates the ability to address the problem of focus in the Applicant's claimed invention.

Once again, this is a clear indication that the rejection is not based on the facts adn evidence but the hindsight given to the Examiner by reading the applicant's specification.

Respectfully submitted,

Dated: January 20, 2004

Ronald Craig Fish
Reg. No. 28,843
Tel 408 866 4777
FAX 408 866 4693

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to: Commissioner for Patents, Mail Stop Amendment , P.O. Box 1450, Alexandria, Va. 22313-1450.

on _____
(Date of Deposit)

Signature of Depositer